**Delegated Credentialing and Recredentialing Policies and Procedures**

**Checklist of Requirements**

Written policies and procedures describing the protection of information including:

* Specific statements about confidentiality
* Release of credentials information to third parties
* Provisions for paper and electronic data management
* Employee orientation and training
* Employee confidentiality agreements
* Disposal of confidential credential information

Written policies and procedures describing the process to select and evaluate practitioners including:

* The types of practitioners to credential and recredential
* The verification sources used
* The credentialing and recredentialing criteria
* The process for making decisions
* The process for managing files (how credentialing information is stored, modified and secured)
* The process to ensure credentialing and recredentialing is conducted in a nondiscriminatory manner
* The process for notifying practitioners if information obtained during the process varies substantially from the information provided by practitioner
* The process for notifying practitioners of the decision within 30-90 (per state regulations) calendar days of the credentialing committee’s decision
* The process to include the Dental Director (or other designated dentist), direct participation in the credentialing and recredentialing program

Written policies and procedures describing the rights of the practitioner including:

* The right to review information submitted to support their application
* The right to correct erroneous information
* The right to receive the status of their credentialing/recredentialing application upon request
* The right to appeal denied participation at the time of initial credentialing/recredentialing

Written policies and procedures describing the composition and role of the credentialing committee including:

* Committee makeup
* Actions that can be taken (approve/deny etc.)
* How participating practitioners provide advice and expertise for credentialing decisions
* The review of credentials for practitioners who do not meet established standards
* The process to ensure that all credentialing/recredentialing meeting standards are reviewed by the credentialing committee, dental director, or designated dentist

Note – committee discussions and decisions are documented in meeting minutes.

Written policies and procedures describing the credentials to be verified including (see separate checklist):

* Current and valid license to practice, (verification time limit - 180 calendar days). Best practice license should not expire within 30 days of committee or conditional approval pending license renewal)
  + Valid DEA or CDS certificate, if applicable. (verification time limit – 180 calendar days not expired at the time of the committee decision DEA waiver if applicable
* Education and training, (verification time limit – prior to credentialing decision)
  + Verify the highest of the education level, board certification, residency, graduation from dental school
* Board certification status, if applicable, verification time limit – 180 calendar days)
* Current malpractice insurance – policy to include required amount of coverage
* Five year work history including explanation for gaps more than 6 months in work history (verification time limit 365 calendar days (may vary by state)
* Last five year history of professional liability claims resulting in settlement or judgment, verification time limit – 180 calendar days
* State sanctions, restrictions on licensure and limitations on scope of practice, verification time limit – 180 calendar days
* Medicare and Medicaid sanctions
* Correctness and completion of the credentialing application\* – See NADP’s Universal Credentialing Application form which includes the attestation questions (Signature date- 180 calendar days)

\*Or credentialing application required by the dental plan, *DSO* or state requirement

Written policies and procedures describing the length of the recredentialing cycle and the elements to be reviewed including (see separate checklist):

* Required every 36 months
* Current and valid license to practice (verification time limit - 180 calendar days. Best practice license should not expire within 30 days of committee or conditional approval pending license renewal)
* Valid DEA or CDS certificate, if applicable (verification time limit - 180 calendar days not expired at the time of the committee decision)
  + DEA waiver if applicable
* Board certification status
* Current malpractice coverage
* Malpractice history
* State sanctions, restrictions on licensure and limitations on scope of practice
* Medicare and Medicaid sanctions
* Updated attestation questions (Signature date- 180 calendar days)
* Tracking and trending of grievance (if applicable by carrier or state)

Written policies and procedures describing ongoing monitoring and interventions including:

* Collection/review of Medicare and Medicaid sanctions
* Collection and review of sanctions and license limitations
* Collection/review of complaints and/or adverse events
* Implementation of corrective actions when instances of poor quality regarding the above is identified

Written policies and procedures regarding the reporting of practitioners to appropriate authorities for quality reasons including:

* The range of actions available to the credentialing committee/organization
* The process for informing practitioners of the appeal process

Written policies and procedures describing the sub-delegation of credentialing activities

* If no credentialing activities are sub-delegated, the policy and process must state as much.

**Written Policies and Procedures describing Credentialing Information Integrity (Formerly Credentialing System Controls)**-Delegated Entity has security controls in place to protect credentialing information from unauthorized modification, whether electronic or paper files. Entity’s policies and procedures describe the process for:

* Limiting physical access to the operating environment that houses credentialing information, to protect the accuracy of information gathered from primary sources and NCQA-approved sources.
* Preventing unauthorized access, changes to and release of credentialing information.
* Password-protecting electronic systems, including user requirements to:
* Use strong passwords.
* Discourage staff from writing down passwords.

User IDs and passwords unique to each other.

Change passwords when requested by staff or if passwords are compromised.

Disabling or removing passwords of employees who leave the organization and alerting appropriate staff who oversee computer security.

* Delegated Entity monitors its compliance with the policies at least annually and takes appropriate action, which includes:

1. Identifying all modifications that do not meet established criteria

2. Analyzing all modifications that do not meet the policies and procedures

3. Taking actions to address all inappropriate modifications.

* When Delegated Entity identifies modifications that do not meet its policies, it implements a quarterly monitoring process to assess the effectiveness of its actions on all findings.
* Annually, Delegated Entity will provide a copy of its’ compliance report and any quarterly monitoring results.
* Organization will evaluate the Delegated Entity’s audit of its compliance with credentialing system security to ensure compliance with the Delegation Agreement. If the Delegated Entity is unable to identify all noncompliant modifications the Organization shall review all modifications made that did not meet the modification criteria allowed. The Organization will use a sampling to identify potential noncompliant changes. Organization will implement a quarterly monitoring process to assess the effectiveness of actions taken to address the findings.

**Credentialing Information Integrity Oversight Audit**  
The System Controls Oversight Audit report is completed by the Director of Operations and Security and Compliance Manager on a semi-annual basis as evidence of monitoring credentialing system controls and to provide documentation of improper modifications.

The organization audits credentialing verifications, decisions, and ongoing monitoring for the following inappropriate documentation and updates:

* Falsifying credentialing dates (e.g., licensure dates, credentialing decision dates, staff verifier dates, ongoing monitoring dates).
* Creating documents without performing the required activities.
* Altering existing documents (e.g., credentialing minutes, clean-file reports, ongoing monitoring reports).
* Attributing verification or review to an individual who did not perform the activity.
* Updates to information by unauthorized individuals.

The audit universe includes practitioner files for all initial credentialing decisions and all recredentialing decisions made or due during the look-back period. The organization randomly audits a sample of practitioner files from the audit universe using 5% or 50 files, whichever is less. The random sample includes at least 10 credentialing files and 10 recredentialing files. If fewer than 10 practitioners were credentialed or recredentialed within the look-back period, the organization audits all files. The organization may choose to audit more practitioner files than NCQA requires.

The organization provides an auditing and analysis report that includes:

* • The date of the report.
* • The title of staff who conducted the audit.
* • The audit method:
* – Audit period.
* – Audit universe size.
* – Audit sample size.
* – File identifier (individual practitioner).
* – Type of credentialing information audited
* • Findings for each file.
* – A rationale for inappropriate documentation and updates.

• The number or percentage and total inappropriate documentation and updates by type of credentialing information.

The organization must provide a completed audit report even if no inappropriate documentation and updates were found.

***Please reference to the NCQA Guidelines for additional details.***